L'INVASIONE DELL'UCRAINA CAMBIA ANCHE IL CYBER RISK

di CINZIA ALTOMARE

QUALI POTREBBERO ESSERE LE CONSEGUENZE DI UN CONFLITTO CHE CRESCE D'INTENSITÀ ANCHE NEL MONDO INFORMATICO? IL SETTORE ASSICURATIVO È PRONTO A FAR FRONTE A UN ALLARGAMENTO DEI CONFINI DEL RISCHIO CIBERNETICO? LA SCARSA CAPACITÀ DEL MERCATO E L'AMPIEZZA DELLA MINACCIA NON LASCIANO BEN SPERARE

Il 6 dicembre 2021, la Corte Suprema del New Jersey ha emesso un primo giudizio a favore di **Merck** (azienda leader nel settore delle tecnologie, con particolare specializzazione nell'healthcare e life science) contro **Ace**, dichiarando che l'esclusione del rischio di guerra contenuto nella polizza emessa da quest'ultima era inapplicabile alla controversia trattata.

Nel 2017 la Merck ha subito perdite per circa un miliardo e mezzo di dollari per danni da interruzione di attività, in seguito all'attacco informatico denominato *Notpetya*, un caso considerato ormai di scuola per gli esperti di cyber risk. Il danno è stato denunciato sulla polizza *all risks* in corso con Ace, all'interno della sezione che copre le perdite derivanti dalla distruzione o corruzione di dati e software dei computer. Gli assicuratori hanno respinto il sinistro in base alla teoria, sostenuta da molti e anche da fonti governative, che il malware Notpetya fosse stato in realtà ispirato o addirittura commissionato dalla Russia. Si sarebbe quindi trattato di un caso di *cyberwar* e ciò comportava l'applicazione dell'esclusione del rischio di guerra e atti ostili, contenuta nella polizza.

LE RAGIONEVOLI ASPETTATIVE

La Corte ha osservato che, pur essendo Merck un'azienda sofisticata e dotata di grande expertise sulle questioni di natura tecnologica, non si poteva per questo considerare che tale esclusione fosse stata effettivamente negoziata dall'azienda, e ha dunque applicato una norma vigente nel New Jersey secondo la quale nei contratti assicurativi devono essere privilegiate le "ragionevoli aspettative dell'assicurato", quando il significato letterale dei termini contenuti in polizza abbiano la valenza di un "comune utilizzo".

Secondo la Corte, le polizze all risks coprono tutti i rischi, a meno che una disposizione specifica non escluda una determinata copertura. Dal momento che non risultava che alcun tribunale avesse applicato un'esclusione del rischio guerra (o atti ostili) a fatti in qualche modo vicini a quelli trattati e che, pur essendo consapevole dell'inasprirsi degli attacchi informatici provenienti da fonti non solo private, ma anche da intere nazioni, l'assicuratore non si era dato pena di rendere più comprensibile il linguaggio della clausola

e di avvisare l'assicurato che intendeva escludere gli attacchi informatici, la Corte ha concluso che Merck avesse il diritto di considerare che l'esclusione presente in polizza si applicasse solo alle forme tradizionali di guerra e non agli attacchi informatici come Notpetya.

LE CONSEGUENZE DELLA GUERRA

La decisione della Corte Suprema del New Jersey si basa essenzialmente su una particolare normativa che interpreta le polizze assicurative a favore degli assicurati, e molti osservatori si chiedono se lo stesso risultato sarebbe stato ottenuto in altri Paesi, soggetti a leggi diverse.
Alla luce di quanto sta accadendo dallo scoppio della guerra in Ucraina, questa decisione assume un interesse particolare, perché si moltiplicano gli interventi di hacker che operano a favore di questa o quella parte, e le compagnie assicuratrici potrebbero non essere ancora pronte a considerare le conseguenze che l'attuale situazione geopolitica può comportare sul piano delle polizze in corso, soprattutto per quanto concerne il cyber risk.

LE ASPETTATIVE (DISALLINEATE) DEI CONSUMATORI

In Europa, questo mercato muove da qualche anno passi stentati, rappresentando una promessa di sviluppo per le compagnie di assicurazione, in contrasto con le tante problematiche tecniche che comporta affrontare un rischio sistemico come questo.


© A.Greeg – iStock

Da tempo, si discute di come il rischio cyber si collochi ai primi posti nella scala delle preoccupazioni che affliggono i risk manager; tuttavia, questo ramo fa grande fatica a decollare, per ragioni che non possiamo certo limitare alla cattiva percezione del rischio stesso o all'endemica tendenza delle aziende a risparmiare sui costi assicurativi. La verità è che l'aspettativa del consumatore è qui assai disallineata dai contenuti delle polizze.
Le ragioni sono diverse e in alcuni casi assai difficili da aggirare. Un esempio tipico è costituito dall'impossibilità a coprire l'ammontare delle multe e ammende comminate dalle autorità garanti (che rappresentano uno dei costi più temuti dalle aziende stesse), all'interno di molti ordinamenti giuridici, tra cui il nostro.

LA SCARSA CAPACITÀ DEL MERCATO

Un altro problema è certamente costituito dalla scarsità di capacità che questo mercato offre: sono assicurate poche centinaia di migliaia di euro per polizza, quando **Mandiant**, ad esempio, valuta intorno ai quattro milioni di dollari il costo medio per ciascun *data breach*. Per le compagnie di assicurazione non è facile offrire massimali ampi, in quanto manca loro il supporto dei riassicuratori, spaventati dall'effetto che questi sinistri potrebbero avere sulla larga scala che caratterizza questi scenari.
Tutti si rifugiano, insomma, dietro limitazioni di copertura che potrebbero consentire loro di giocare su questo tavolo, ma che d'altro canto risultano forse troppo restrittive per chi deve fronteggiare perdite che possono ammontare facilmente a svariati milioni. Ci sono però altre questioni che non sono meno problematiche.

IL CASO KASPERSKY

Prendiamo ad esempio il caso del software **Kaspersky**, del quale gli esperti discutono da diverse settimane. Questo antivirus è prodotto da un'azienda con sede legale in Russia, il cui ceo e fondatore pare abbia avuto relazioni e legami con il **Kgb**. E se pensiamo al Kgb, non ci viene in mente soltanto la nazione russa, ma **Vladimir Putin** in persona.
Per l'Italia si tratta di prendere posizione contro l'uso di Kaspersky, in quanto associato a un Paese ora nemico, che nel recente passato è stato accusato di avere intrapreso iniziative aggressive, in termini di cy-

berwar. Si sospetta la presenza di uno *spy software* al suo interno e **Franco Gabrielli**, sottosegretario alla Presidenza del Consiglio con delega alla sicurezza nazionale, ha invitato a prendere le distanze dal suo utilizzo, chiedendo di eliminarlo dai server della pubblica amministrazione e anticipando la promulgazione di un decreto specifico a questo scopo. Il 18 marzo scorso è stata aperta anche un'istruttoria dal *Garante della privacy*.

In Italia, il software è utilizzato da circa 2.700 uffici pubblici, tra ministeri, Comuni, forze dell'ordine e aziende private. È dunque possibile che questo antivirus contenga un software spia o una *backdoor* infiltrata per opera del governo russo?

LE PRESSIONI DEL GOVERNO RUSSO

Il 27 febbraio scorso, **Stefano Quintarelli**, informatico, ex deputato e da sempre in prima linea sul fronte dell'innovazione digitale nella pubblica amministrazione (è l'ideatore dello *Spid*), ha firmato un articolo su *Il Post*, nel quale introduce una discussione sul rapporto tra il software antivirus Kaspersky e l'Italia. A esso è seguita un'interrogazione parlamentare da parte del Gruppo Misto alla Camera dei deputati. Capire quanto sia grave questa faccenda è davvero arduo, perché questo software è ormai utilizzato da diversi anni nella pubblica amministrazione italiana. Inoltre, qualsiasi software è sempre riconoscibile: ciò vuol dire che non è necessario leggere il cosiddetto *codice della sorgente*, per studiare il comportamento di questi programmi durante la loro esecuzione.

Infine, la Kaspersky è una multinazionale assai strutturata, che ha dislocato i suoi *datacenter* dedicati ai clienti europei in Svizzera e ha sempre fornito garanzie di sicurezza considerate, fino a questo momento, più che sufficienti.

Ma la crisi prodotta dall'invasione dell'Ucraina ha incrementato le preoccupazioni nei confronti di questo antivirus, nel timore che l'attuale governo russo possa fare pressione sull'azienda produttrice, al fine di operare del sabotaggio o spionaggio informatico contro i suoi clienti, ubicati in paesi non più vicini o alleati con la Russia.

LIBERARSI DELLA DIPENDENZA TECNOLOGICA

Questo scenario vedrebbe il diffondersi di una grave minaccia informatica mirata nei confronti delle strutture critiche italiane, agendo con tutte le capacità di un malware ed eventualmente estraendo dati riservati verso un paese nemico. La dipendenza dalla quale dobbiamo liberarci non è dunque limitata alla questione energetica, ma riguarda anche la tecnologia russa, per evitare che da strumento di protezione questa possa trasformarsi in un arnese di attacco.

Quali potrebbero essere le conseguenze della questione sul piano assicurativo è poi davvero complicato da immaginare. Negli anni più recenti, in Italia, le esclusioni del rischio guerra (o atti ostili) sono state utilizzate senza troppa convinzione dalle compagnie, forti dello stato di pace che per fortuna ha interessato per lungo tempo il Paese.

Di fronte alla possibilità di un'escalation che potrebbe facilmente trasformare il cyber risk da rischio sistemico a rischio ingestibile, quale sarà la reazione dei player di un mercato che è già accusato di essere asfittico e non sufficientemente equipaggiato per affrontare il contesto attuale?